NHB 1700.1(V3)

NASA SAFETY MANUAL

48 P

VOLUME 3

SYSTEM SAFETY

(NHB-1700.1(V3)) NASA SAFETY MANUAL. VOLUME 3: SYSTEM SAFETY (NASA) 48 p

N94-70730

Unclas

Z9/81 0190962

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

PREFACE

DATE: March 6, 1970

This Volume 3 of the NASA Safety Manual sets forth the basic elements and techniques for managing a system safety program and the technical methods recommended for use in developing a risk evaluation program that is oriented to:

a. The identification of hazards in aerospace hardware systems.

b. The development of residual risk management information for the program manager that is based on the hazards identified.

The methods and techniques described in this volume are in consonance with the requirements set forth in NHB 1700.1 (VI), Chapter 3.

This volume and future volumes of the NASA Safety Manual shall not be rewritten, reprinted or reproduced in any manner. Installation implementing procedures, if necessary, shall be inserted as page supplements in accordance with the provisions of Appendix A.

No portion of this volume or future volumes of the NASA Safety Manual shall be invoked in contracts.

Comments and questions concerning the contents of this publication should be referred to the National Aeronautics and Space Administration (NASA Safety Office, Code DY), Washington, D.C. 20546.

NASA Acting Director of Safety

DISTRIBUTION:
SDL 1(SIQ)

PAGE _____ INTENTIONALLY BLANK

ORGANIZATION OF THE NASA SAFETY MANUAL

OVERALL COVERAGE

The NASA Safety Manual will be issued in several volumes, by major safety subject breakdowns. The following list shows the initial plan for publishing the individual volumes:

Volume	Title	Assigned No.
1	Basic Safety Requirements	1700.1(V1)
2	Reserved	
3	System Safety	1700.1(V3)

DOCUMENT REFERENCING

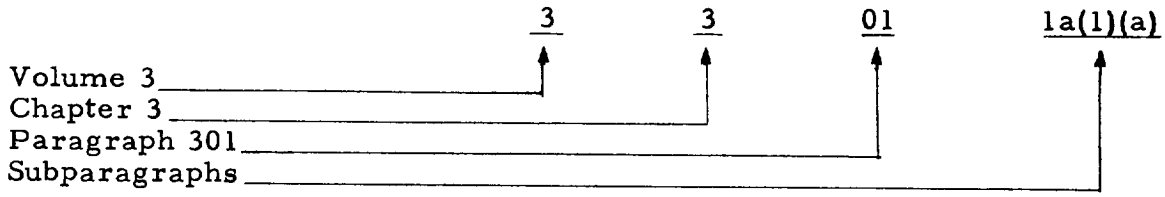
Each volume is assigned its own identification number within the basic classification code. The alpha-numeric suffix within a parenthesis identifies the volume of the manual; e.g., NHB 1700.1(V3): this number indicates that this is the third volume.

When a volume is revised, the suffix identification will be changed to indicate the revision number such as NHB 1700.1(V3-A).

In referencing or requesting any volume of the NASA Safety Manual, the complete, specific NHB number must be used.

PARAGRAPH REFERENCING

1. Within the NASA Safety Manual. The following shows the general paragraph numbering system applicable to all volumes:



This system provides for referencing any paragraph or complete volume requirement in any other volume of the NASA Safety Manual without the need for identifying the NHB number and title.

2. In Other NASA Documents. When it is necessary to reference any paragraph in any other NASA document, the specific NHB number and paragraph number must be used together as follows: "NHB 1700.1(V1), par. 1103-1a (1)(a)," or "paragraph 1103-1a(1)(a) of NHB 1700.1(V1)." When it is necessary to reference any complete volume in any other NASA document, the specific NHB number (which also identifies the volume) must be used.

TABLE OF CONTENTS

CHAPTER 1: MANAGEMENT TECHNIQUES

3100 INTRODUCTION

There is direct relationship between the degree of safety achieved in a NASA aerospace system and the management emphasis placed on the safety of the system being designed, manufactured, tested, and operated. This chapter of the safety manual describes the tasks that should be accomplished and the working relationships that should be established to formalize the system safety effort into a discipline, to the end that the program manager will have maximum visibility into the risks he is assuming.

3101 PURPOSE AND SCOPE

This chapter provides functional safety managers with an outline of the techniques that are useful in the planning, implementation, and administration of a system safety program. The management techniques described are applicable to any size or type of NASA hardware development program and throughout the entire system life cycle. These methods should be implemented to the extent that the evolving system safety effort fully supports the unique needs of the hardware program. This Volume is intended to be evoluntionary in nature and therefore subject to continuous upgrading and change as new methods are developed and have been proven satisfactory for NASA application.

3102 RISK EVALUATION

1. The program manager of an aerospace system must assume certain risks that are attendant to the design, manufacture, test, and operation of the hardware system to effectively accomplish the mission for which the system was developed. The acceptance of these risks should be based on thorough visibility as to the nature of hazards and risks that are in existence and the options and alternatives to the acceptance of the risks.
2. The decision on whether to assume a risk is clearly a program management responsibility. This decision is no better than the quality of the risk data that serves as a basis for the decision. Accordingly, the development of hazard and risk data should be assigned as a responsbility to professionals whose training and orientation cause them to search out and find the hazards in the system before these hazards manifest themselves in terms of damaged or destroyed hardware.

3103 SYSTEM SAFETY PROGRAM ELEMENTS

1. Each functional system safety program has nine basic elements which include:
   a. Planning,
   b. Organization,
   c. Contracting,

d. Interface/Coordination,

e. Criteria,

f. Analysis,

g. Reporting,

h. Evaluation,

i. Data Retention.

2. Each of the above elements and the related activities are described in the ensuing paragraphs. All of these elements are oriented toward an overall approach to risk evaluation by:

a. Identifying the hazards in the system.

b. Determining corrective actions that may be implemented to either remove, or control, the hazard or to provide alternatives.

c. Recommending corrective action or alternatives to the appropriate management level for a decision to either resolve the hazard or assume the risk.

d. Documenting those areas in which a decision has been made to assume the risk, including the rationale for the risk assumption.

3. The detail with which each of the nine safety program elements set forth in subparagraph 1. is developed and implemented is dependent upon the complexity and mission of the hardware system being developed.

3104 PLANNING

1. PRELIMINARY SAFETY TASKS

It is anticipated that, in most cases, formal planning of the safety effort for support of the system feasibility studies would not be initiated. There are, however, several typical safety tasks that should be completed during these activities. These tasks then become the foundation for the planning of system safety efforts during the system definition, design, manufacture, test, and operation. These include:

a. A review of pertinent historical safety data from similar systems.

b. A continuing review of the gross hardware requirements and concepts, to maintain an understanding of the evolving system.

c. A review of the proposed mission objectives.

d. Completion of the planning for follow-on safety activities.

e. The completion of preliminary hazard analyses to identify potentially hazardous systems and to develop initial safety requirements and criteria.

f. Participation in trade studies with the result of the preliminary hazard analyses identifying highly hazardous areas, with recommendations as to the alternatives.

g. Identification of the requirement for special contractor safety studies that may be required during system definition or design.

h. Estimation of gross resource requirements for the system safety program during the complete system life cycle.

i. Preparation of an index document that identifies all pertinent safety data developed during the life cycle of the system, such as the results of analyses, the criteria and requirements implemented, the results of special studies and the applicable historical data. This index is updated at the conclusion of each major increment of the system development or as determined by program milestone dates.

2. GOALS AND OBJECTIVES

a. Any planning exercise requires that certain basic decisions be made. Safety goals and objectives should be established, and the type of system safety input that is to be furnished to the overall program should be determined prior to initiating the planning effort. Goals should be measurable in every case and should state what system safety would intend to accomplish as a result of having performed the various safety tasks.

b. Once these safety goals and objectives have been established and agreed upon by appropriate program management level, the planner can begin to become familiar with both the evolving hardware system and the environment within which the safety program is to be conducted. Having equated the safety goals to the needs of the system being developed, the planner considers all the alternative methods and analyses that can be used to meet these safety goals and objectives. The optimum methods are selected from these alternatives and the planning is begun. It should be noted that these goals must be structured such that safety tasks can be selected that will accomplish the goals and when the tasks have been completed the result of the effort will clearly demonstrate that the goals have been met.

3. PLAN CONTENTS

The Safety Plan should include:

a. A description of the initial safety tasks initiated during the feasibility studies, system definition, design, manufacture, test or operation that are to be continued throughout the forseeable future of the system life cycle.

b. Additional tasks that are to be initiated during ensuing program activities that evolve from the list of safety elements described in paragraph 3103.

c. The development of requirements for contractor safety effort.

d. An estimate of numbers and types of personnel required for the safety effort.

e. A description of the methods that will be used to perform these safety tasks, control the effort and accomplish the objectives.

f. Scheduling the safety effort including milestone identification, program activities, phasing, and integration.

g. Identification of the safety output that will result from the effort, the expected application of the output, with provisions for the documentation of specific results of the safety effort.

A typical safety plan outline is shown as Figure 1.

4. PLAN REVISIONS

a. It should be noted that if the planned safety program is to have sufficient flexibility, the individual plan must be revised as required to satisfy the changing needs of the program, although the plan should not be revised for the sake of change alone. Further, it can readily be seen that a plan may vary in size from one page in length to a detailed multi-page document, depending on the size, complexity and needs of the system.

b. The planning tends to be an iterative process in that the plan is refined and expanded as milestones of the system development are accomplished. Emphases are realigned, nonproductive tasks are abandoned and new tasks developed as required to accomplish the safety goals. Analysis methods are evaluated against program needs and specific techniques are selected and implemented, as required to provide a sufficient depth of safety/risk evaluation visibility.

3105 ORGANIZATION

1. The organization of the functional system safety effort is developed to accomplish the tasks set forth in the safety plan. Safety may be part of the system engineering organization or part of a systems effectiveness organization, collocated with the reliability, quality or maintainability organizations. As a general rule, to maintain objectivity and the check and balance system, it is preferable that system safety not be part of the design engineering organization.

2. The major safety tasks to be accomplished are broken down into subtasks and responsibilities assigned that will support accomplishment of the safety goals. The ongoing activities, together with the quantity and complexity of the safety tasks scheduled for completion, dictate the size and technical depth of the safety organization. For example, a safety organization may vary from only one man who spends part of his time accomplishing the safety tasks to an organization of 20 or more people supported by an extensive contracted effort. Obviously good staffing practices should be followed, and the greatest possible technical professionalism developed.

CHECKLIST OF REQUIREMENTS FOR A SYSTEM SAFETY PLAN

1.0 PURPOSE AND SCOPE

2.0 APPLICABLE DOCUMENTS

(Reference only documents cited in the plan text)

3.0 SAFETY ORGANIZATION

- 3.1 Relationship to total organization
- 3.2 Organizational array
- 3.3 Responsibilities
- 3.4 Interfaces

4.0 SAFETY TASKS TO BE COMPLETED

- 4.1 Criteria development
- 4.2 Analyses
- 4.3 Design/program review participation
- 4.4 Contractor/subcontractor requirements
- 4.5 Reporting
- 4.6 Documentation
- 4.7 Planning
- 4.8 Evaluations

5.0 METHODS FOR ACCOMPLISHING SAFETY TASKS

- 5.1 Criteria - development, documentation and monitoring
- 5.2 Analysis technique
- 5.3 Other program activities

6.0 SCHEDULE FOR TASK COMPLETION

(Keyed to major program milestones)

Figure 1

3. Irrespective of the relative size of the safety organization, it should be placed in the reporting chain at a point which allows the risk evaluation output resulting from the safety effort to flow directly to the appropriate level of management in support of risk management decisions.

3106 CONTRACTING

1. TWO FORMS

Contracting of a system safety effort may take one of two forms. The effort may be contracted in a separate contract, such as a special safety study during the early development, or may be part of the total system procurement package. In either case, unless the requirements being contracted are carefully prepared so that the contractor clearly understands what he is expected to accomplish, the contractor cannot provide the engineering and management services being sought. The fundamental elements of the two forms of procurement mentioned above are essentially the same and follow a well-defined procurement system (see NASA Procurement Regulation, Subpart 52 - SAFETY).

2. THE REQUEST FOR PROPOSAL (RFP)

The RFP must state in clear, concise terms:

a. The scope of the effort.

b. The specific tasks the contractor is expected to perform.

c. The reporting requirements.

d. The program milestones that must be met.

e. That the contractor is expected to provide a system safety plan as part of his bid package, which is in consonance with paragraph 3104. This contractor plan should include a listing of the system safety tasks he plans to complete and include a description of:

(1) The methods he plans to use in accomplishing these tasks.

(2) The output or product that will be produced by the safety effort.

(3) The use that will be made of the safety output.

(4) The organization that will be developed to complete the task.

(5) The deliverables.

(6) The reporting of safety problems, activities, and accomplishments.

(7) The sub-tier schedule of activities leading to task completion in support of major program milestones.

3. PROPOSAL EVALUATIONS FOR SOURCE SELECTION

The safety manager should participate in the proposal evaluation activities and rate each proposal on the basis of the contractor's demonstrated understanding of the RFP requirements reflected in his plan as well as the cost history and the history of the contractor's past performance.

4. THE STATEMENT OF WORK

The evaluation of the proposal should also lead to the decision on the suitability of the contractor's system safety plan for use as a segment of the overall statement of work. Normally a separate segment of the statement of work covering the system safety requirements, included in the contract schedule, is preferable to negotiation of the contractor's safety plan since the contractor's plan is his blueprint for meeting the requirements. This segment of work may be based on the original RFP and the safety data submitted by the contractor as part of his bid package.

3107 INTERFACE/COORDINATION

1. GENERAL

The effectiveness of the functional system safety effort is determined by the quality and quantity of the output and how that output is applied. The development of the output is dependent upon the interfaces established, the currentness and quality of the data safety personnel have to work with, and the technical competence within the safety organization.

2. INTERFACE ESTABLISHMENT

Working interfaces should be established at the earliest possible time in the system development and should be postured on the basis that system safety has a valuable service to provide the other organizations in the program. As each interface is established, the safety manager should strive to reach an understanding with his counterparts as to:

a. The type of data that is to be produced by each organization.

b. The amount of this data that will be needed by safety personnel and a schedule for its availability.

c. The use safety personnel will make of this data.

d. The output of the safety effort including the format and availability schedule.

e. The safety data or effort that may be required by the interfacing organizations.

Typical interfaces and data flows are pictured in Figure 2, which shows the safety activity set apart on the left in order to better describe the data exchange.

SAFETY INTERFACES AND TYPICAL DATA FLOW

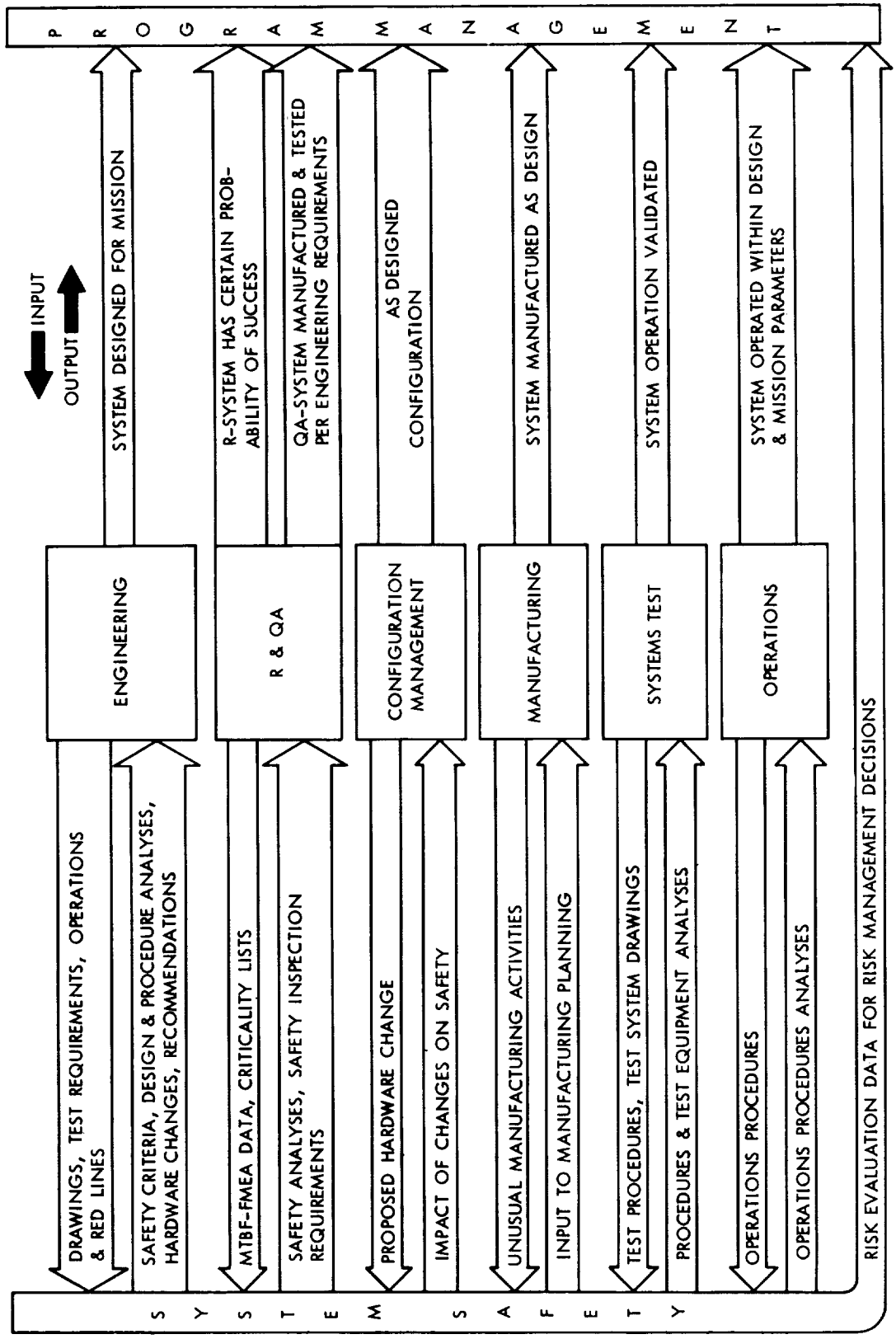


Figure 2

3. THE SAFETY-ENGINEERING INTERFACE

The interface with engineering is especially important. This working relationship should be developed during the early part of the system development and continued throughout the life cycle to the conclusion of the program. System safety personnel work closely with engineering personnel in developing safety criteria, and, based on the safety analysis, recommend methods of reducing risks, coordinate on the design of safety devices and recommend hardware changes to remove or control hazards. Safety personnel provide close support and assistance to the engineering staff during design and program reviews, and, as the result of having performed a thorough technical safety effort, should be able to make a significant contribution during these reviews in terms of visibility into the risk assumption status.

4. THE SAFETY-R & QA INTERFACE

a. The system safety-reliability and quality interface is of particular interest because the two areas can provide effective support to each other when properly conducted. Much of the data developed by the reliability program finds use by the functional safety effort in the preparation of the Safety Analyses, and there are common interests between the two programs in design review, failure reporting and human error areas. It is therefore important that the two areas coordinate closely with one another in program planning and execution to ensure that each provides appropriate support to the other and that duplication is eliminated.

b. The safety effort should provide the quality assurance organization with inspection requirements for safety items and information on safety critical characteristics. A rapid flow communication channel should be established and maintained to assure that the safety staff receives quick notification of safety discrepancies, parts failures and assembly errors.

5. THE SAFETY-CONFIGURATION MANAGEMENT INTERFACE

The safety-configuration management interface should be established as soon as the design of the system is sufficiently well defined to be controlled by a configuration management activity. Safety personnel should review all changes for their potential impact on the safety of the system. Safety changes especially should be reviewed to determine that they do improve the safety and reduce the risk sufficiently to merit implementing the change. The safety organization also should participate in all proposal and committing change board activities when safety changes are being exercised.

6. THE SAFETY-MANUFACTURING INTERFACE

a. The system safety-industrial safety working relationship is established in the manufacturing, test and operations areas. The system safety-manufacturing relationship can best be characterized as advisory in nature, depending largely on the relative effectiveness of the industrial safety program.

b. The system safety organization should review the manufacturing planning of critical activities to assure that a fabrication or assembly process does not exist that can result in residual damage being incorporated into the system as part of the manufacturing process.

c. Major reliance is also placed on the quality control activities during the manufacture of the system. Requirements for special inspection of safety critical items and activities should be included on the proper drawings. These safety items are then inspected by the quality people as part of their regular inspection and buy-off activities with failure and rejection reports providing a rich source of useful safety data.

7. THE SAFETY-SYSTEMS TEST INTERFACE

a. The system safety staff works closely with the test organization. Test procedures are reviewed to assure that hazardous tests are identified as such and that the procedures, prepared to operate the system under test, contain shutdown and backout capability as well as cautions and warning notes.

b. Test systems are analyzed to assure that hazards have been fully considered and that the risks are minimized wherever possible. Safety representatives should occasionally witness the accomplishment of hazardous testing to measure the validity of the safety input to the test procedures and to gain a better understanding of the test activities.

8. THE SAFETY-OPERATIONS INTERFACE

a. The safety activities completed during operation of the system include staff support during system final assembly, checkout and validation, maintenance and operation. Hazardous tasks performed as part of the checkout and launch are identified as such, and the supporting contingency planning is reviewed thoroughly to assure that exposure is minimized and recovery is well organized and planned.

b. Operating procedures are reviewed to assure that backout or shutdown provisions, warning and caution notes have been included.

c. Special attention is devoted to system interfaces since hazards recognize neither contract nor mechanical boundaries. The safety staff can make a major contribution to the system integration activities as a result of having completed the normal safety tasks.

d. The participation of safety personnel in system operations should be on an active basis, to measure the validity of the safety input to the operations procedures and to become more familiar with the operational program.

9. SYSTEM SAFETY-PROGRAM MANAGEMENT INTERFACE

a. The effectiveness of the system safety effort is measured in terms of the safety impact on the system from the standpoint of reduced risks. One of the principal avenues available to exert this influence on the system is through the program manager's decisions. Accordingly, the safety manager must establish an effective interface with the program manager so that the program manager will understand what kind of an output can be expected from the system safety effort, when this output will be received, and how it will be useful to him. Next, safety personnel must mount a competent effort to produce a technically accurate output which is acceptable to both engineering and the program manager from a technical standpoint.

b. The provision of this safety output, in the main, should be scheduled to the major program decision points such as the Preliminary Design Review (PDR), First Article Configuration Inspection (FACI), Design Certification Review (DCR), Flight Readiness Review (FRR) and any other special reviews. The safety output should be expressed as a total risk profile with sufficient supporting data to enable the program manager to decide whether to:

(1) Assume the risks;

(2) Change the hardware to reduce the risks; or

(3) Revise the mission to reduce the exposure of the hardware and thereby reduce the risks, or by imposing constraints at control exposure to high risks.

c. The safety manager should evaluate the output produced by the effort performed in the name of safety on a continuing basis to assure that it is useful, and that it is being used. This provides a valuable control function to delete nonessential tasks from the on-going safety activities.

10. OTHER INTERFACES

Where more than one field installation is involved in conducting the system development and operation, it is vital that interinstallation safety coordination meetings be held on a regularly scheduled basis and that communication channels be opened and encouraged for the expedited flow of safety data. This same type of safety data exchange system should be used in the case where more than one prime contractor is used by an individual field installation.

3108 CRITERIA

1. GENERAL

The second method by which the system may be influenced in addition to "through the decision process" (see paragraph 3107-9) is by means of the criteria and requirements specified for the design, development and operation of the system. Accordingly, special attention should be devoted to the system criteria development process.

2. DEVELOPMENT

Criteria are originated from the results of the safety analyses and from the experience gained from other programs using similar systems. The process is described in Figure 3 and is repetitive in nature to the extent that the criteria are evolved, imposed, and then evaluated for effectiveness on an iterative basis. Any requirement for which several waiver requests are received should be evaluated to determine the practicality of relaxing the requirement. Otherwise, waivers should be granted on a one-time-only basis. When a waiver is granted, the information should be documented as a matter of permanent record, with the reason or the justification for granting the deviation also recorded. It cannot be emphasized too strongly that each waiver may constitute an increase in the risk being assumed and each deviation must be evaluated on its own merits. In any case, waivers should be kept to a minimum.

3. DOCUMENTATION

All safety criteria and safety-related criteria should be recorded in one document which is maintained on an up-to-date basis to show how the requirements were developed and their current state of implementation. Also, the waiver system should be maintained on a very formal basis with each waiver and the circumstances of its issuance fully documented.

3109 ANALYSIS

1. System safety analyses are performed for the purpose of identifying hazards and establishing risk levels. Further examination will reveal that in support of this concept, the analyses perform five basic functions:
   a. Provide the foundation for the development of safety criteria and requirements.
   b. Determine both whether and how the safety criteria and requirements provided to engineering have been included in the design.
   c. Determine whether the safety criteria and requirements created for that design have provided adequate safety for the system.
   d. Provide part of the means for meeting pre-established safety goals.
   e. Provide a means of demonstrating that safety goals have been met.
2. A very strong case can be made for the performance of safety analyses on any system, and all too often the decision on undertaking the effort is resolved down to a matter of economics. It is always necessary to be prudent in the allocation of resources for any effort. From the standpoint of safety analyses, economy should be based on the selection of the appropriate analysis techniques to be used, based on the requirements of the system, and the need for risk visibility. Economy should never be based on the performance of no safety analyses since the absence of analyses results in very little visibility for the program manager as to the actual risk assumption status.

SYSTEM SAFETY ACTIVITIES FUNCTIONAL FLOW

IDEALIZED FUNCTIONS FOR NEW PROJECTS

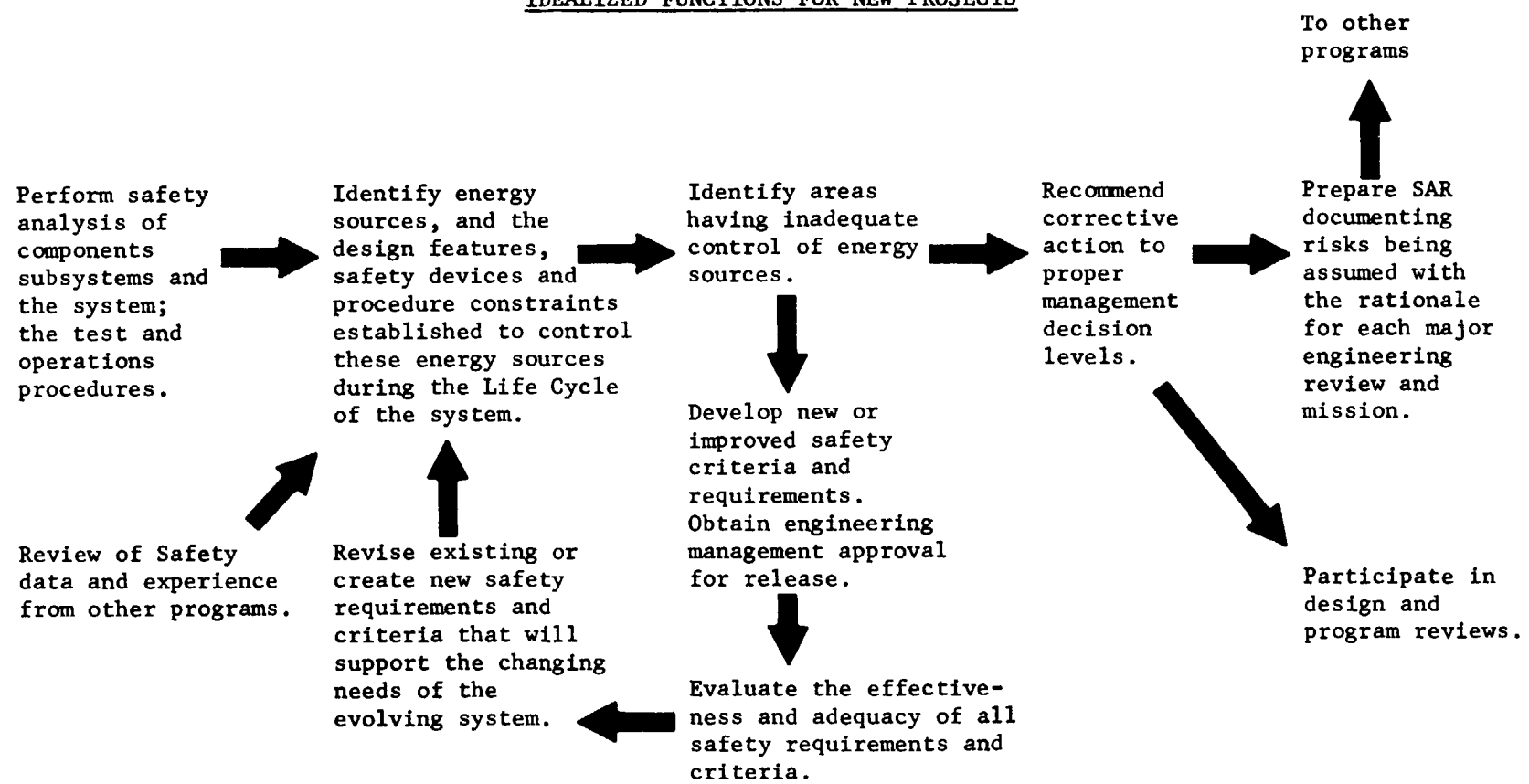


Figure 3

3110 REPORTING

1. DEFINITION OF REQUIREMENTS

The requirements for reporting of progress, hazards and activities should be defined in the various safety plans and/or contracts.

2. GENERAL REPORTING

General reporting covers progress of the effort, milestones attained, and significant accomplishments such as hazards identified and resolved. This type of reporting generally flows in consonance with overall program reporting channels.

3. PROGRAM REVIEWS

Safety inputs to program reviews relative to the risks being assumed and the status of hazard resolution are usually construed as a type of reporting. This type of reporting is formalized around the individual program review format.

4. SAFETY ANALYSES REPORT (SAR)

The SAR, or an input to the SAR, should be prepared in support of each major engineering review and prior to beginning each mission. The requirements for the SAR are contained in paragraph 1310, and include such things as:

a. Risk levels, in terms of risks being assumed.

b. Rationale for the assumption of these risks and the alternative considered.

c. Waivers to safety criteria that have been granted.

d. System safety activities that are behind schedule and have not been completed.

These SAR's serve as a total record of the risks assumed in order to complete each mission.

3111 EVALUATION

1. PURPOSE

The evaluation of a system safety program is performed in order to determine that:

a. The safety management system is properly structured.

b. There is good access to both the system data and the proper management reporting level.

c. The safety goals are being met and the planned tasks are being accomplished and are on schedule.

d. There is an output resulting from the system safety effort.

e. Effective use is being made of safety output.

2. METHOD

a. The evaluation of a safety program is begun by planning the review. The system safety requirements that have been imposed on the organization are determined and a copy of the organization's safety plan is obtained. In general, the most satisfactory approach is to measure the performance of the effort (what is being accomplished) against the approved plan (what was intended to be accomplished). Also an evaluation should be made as to whether the plan itself is current and still responsive to program needs.

b. A checklist similar to the one shown in Figure 4 is a valuable tool for recording the relative acceptability of the various parts of the program. The numbers on the left of the checklist refer to chapters in NHB 1700.1(V1). Special attention should be devoted to areas of effort receiving inadequate attention or the accomplishment of nonproductive or redundant effort.

c. The evaluation should include a discussion with the program manager to assess:

(1) The quality of the output from the safety effort that reaches the program manager.

(2) Whether this output arrives in time to be useful to the program manager.

(3) How the program manager uses this safety input.

(4) How the safety output can be improved and made more useful to the program manager.

d. Upon completion of planning, the organization that is to be reviewed should be notified of the forthcoming evaluation and what is to be covered in the assessment sufficiently well in advance so that proper preparations and coordination can be completed. The evaluation begins with an initial briefing to the appropriate management level that introduces the review team, covers the purpose of the review, identifies what is to be evaluated and assures a debriefing at the conclusion of the review.

e. The review is completed according to plan and the debriefing is completed whenever possible with the same management people as participated in the entrance briefing. The purpose of this debriefing is to come to an understanding of both the good things that were found and the areas requiring increased emphasis or improvement.

f. The report of the evaluation is coordinated with the reviewed organization prior to publishing it, so that any discrepancies, misunderstandings, or inaccurcies can be resolved.

SAFETY EVALUATION CHECKLIST		Organization Reviewed	
DESCRIPTION	RATING: Enter A-Acceptable; R-Recommendation; N-Not Fully Evaluated		
NAME OF EVALUATOR			
Date			
1 Management- ment	a. Attention to Safety		
	b. Delegation and Authority		
	c. Scope of Involvement of Organization		
	d. Organizational Relationships		
	e. Documentation of Policies and Requirements		
	f. Staffing		
	g. Motivation and Promotion of Safety		
	h. In-house Evaluations		
	i. Participation of Safety Office		
	j. Risk Assessment Attitude		
	k. Emergency Planning		
	l. Standards		
	m. Permits/SOP's/Readiness Reviews		
	n. Safety Program Planning		
2 Contracts	a. Adequacy of Procurement Requirements		
	b. Participation of Safety in Procurement		
	c. Evaluation of Contractor Performance		
3 System Safety	a. Criteria-Documentation/ Compliance/Waivers		
	b. Working Interfaces		
	c. Participation in Design/Program Reviews		
	d. Change Evaluation		
	e. Reporting System		
	f. Safety Analyses/Hazard Identification		
	g. Safety Analyses Reports (SAR)		
	h. Nuclear Safety		
	i. Safety Outputs		
	j. Program/Project Review and Evaluation		
	k. Life Cycle Coverage		
4 Safety Skills	a. Certification		
	b. Overall Training Program		
	c. Up-grading Staff Skills		
8 Hazards Identifi- cation, Safety Re- search & Data	a. Hazard Identification		
	b. Safety Research		
	c. Technical Data		
9	ACCIDENT/INCIDENT/MISSION FAILURE INVESTIGATION AND REPORTING		

Figure 4

3. SCHEDULING

Reviews should be completed on a regularly scheduled basis, usually once a year. More frequent evaluations should be scheduled only when the review indicates a problem of major proportions that cannot be resolved with less emphasis than the forcing function of a major review.

3112 DATA RETENTION

1. As a result of having performed the safety activities described in this volume, extensive system safety data will have been developed, including:

   a. Criteria and requirements.

   b. Safety study reports.

   c. Other reports, progress/activity.

   d. Safety analysis reports.

   e. Analyses.

   f. Hazards reports.

   g. Accident reports.

2. These items are valuable safety data that may have application to other systems that are presently being developed, or will be developed in the future, and as such these data should be documented for retention as they are prepared.

3. An up-to-date index of these data should be maintained for each program that identifies this information by report number, title, date of final issue, location, and a pertinent summary abstract so that the data are readily available for use when needed.

CHAPTER 2: TECHNICAL METHODS

3200 INTRODUCTION

The formalization of the system safety activities in the hardware/software development programs of NASA requires as a prerequisite the selection of certain technical methods that are generally accepted as the tools of that specific technology. It is recognized that only a certain amount of basic data evolves as a hardware system is developed. These are the approved engineering drawings and specifications, together with hardware test results, and it is from these basic data that all ancillary data are created. It therefore becomes a matter of major importance as to how these basic data are used and in what manner the data are processed by the various supporting disciplines to accomplish their respective missions. This chapter contains a brief description of those methods that experience has proven to be most effective for use in processing the basic engineering data and applicable ancillary data into risk evaluation information.

3201 PURPOSE AND SCOPE

1. This chapter describes in broad terms the technical system safety methods that are available to a NASA program or system safety manager for use in accomplishing a risk evaluation program. The methods have been described in sufficient detail to provide understanding of the techniques and permit an evaluation of the analysis results. This document does not provide detailed instructions on these methods sufficient to permit the use of this Handbook alone to perform these analyses. Hazard analysis reference publications and training courses are set forth in Appendixes B and C, respectively.

2. The methods described herein are applicable to all NASA hardware systems. The analysis methods may be expanded, reduced or altered as required to suit the specific needs of any separate program, or initiated during any time in the system development, thus assuring maximum flexibility. Further, these methods are not restricted exclusively to system safety and should be considered for applicability to the industrial, public, and aviation safety activities.

3. The reason for undertaking a program of safety analysis is to identify the hazards in a system. Once identified, these hazards are evaluated, first in terms of the relative severity of the hazard, which is the effect the hazardous event would have on the system should the event occur and cause the system or an energy source to go out of control. Secondly, the hazards are evaluated in terms of the exposure of the total system or the time interval during which the hazardous event can affect the system, considering also the location of the hazard in the system. Thirdly, the hazard is evaluated in terms of the likelihood that this event will occur, and, if determined quantitatively, may be expressed by means of probability calculations.

4. The safety analyses are then reapplied to systematically search for the alternatives to assuming excessively high risks during the testing or operation of the system.

3202 HAZARD ANALYSES

1. The following analytical techniques are described in their logical order of application during the system development life cycle, as shown in Figure 5. The first method is the Preliminary Hazard Analysis, which is used in the early phases of the development to identify the energy sources being considered for use in the evolving system, together with the methods selected for the control of these energy sources.

2. As the system becomes better defined and more detailed design data evolve, the Fault Hazard Analysis can be undertaken. This analysis addresses the system down to the piece-part level, if necessary, and should include such items as mechanical linkages, wiring and ducting which connect the critical system elements or components.

3. The final analysis recommended for the more complex systems is the Logic Diagram Analysis which is used to identify critical failure paths. This analysis may be made quantitative using the Fault Tree Technique should the program manager require this amount of visibility.

4. Finally, manufacturing, test and operating procedures should be reviewed (Procedures Analysis) to assure that they are fully annotated with cautions and warning notes and that their use does not initiate any out-of-sequence events.

3203 PRELIMINARY HAZARD ANALYSIS

1. Usually the first analysis technique applied in a typical system development program is a preliminary hazard analysis based on descriptions of mission functions or events to be achieved. A preliminary analysis is performed by applying data obtained on previous programs from systems analogous to those defined generically from the descriptions of subsystems considered for use in accomplishing mission functions. The purpose of this analysis is to identify safety critical areas and the hazards involved in the mission(s) under consideration and provide management with risk visibility during either feasibility studies or system definition activities. This preliminary analysis provides a comprehensive listing of hazards commensurate with the generic system(s) defined. The comparative data utilized from analogous systems in previous programs reflect the results of potential hazards identified from analyses and experience with those hardware systems, with emphasis on all aspects of these systems and their usage.

2. The preliminary hazards analysis should include:

   a. A review of all pertinent safety data produced by other NASA systems to take advantage of previous safety experience.

SAFETY ANALYSIS - PROGRAM ACTIVITY RELATIONSHIP

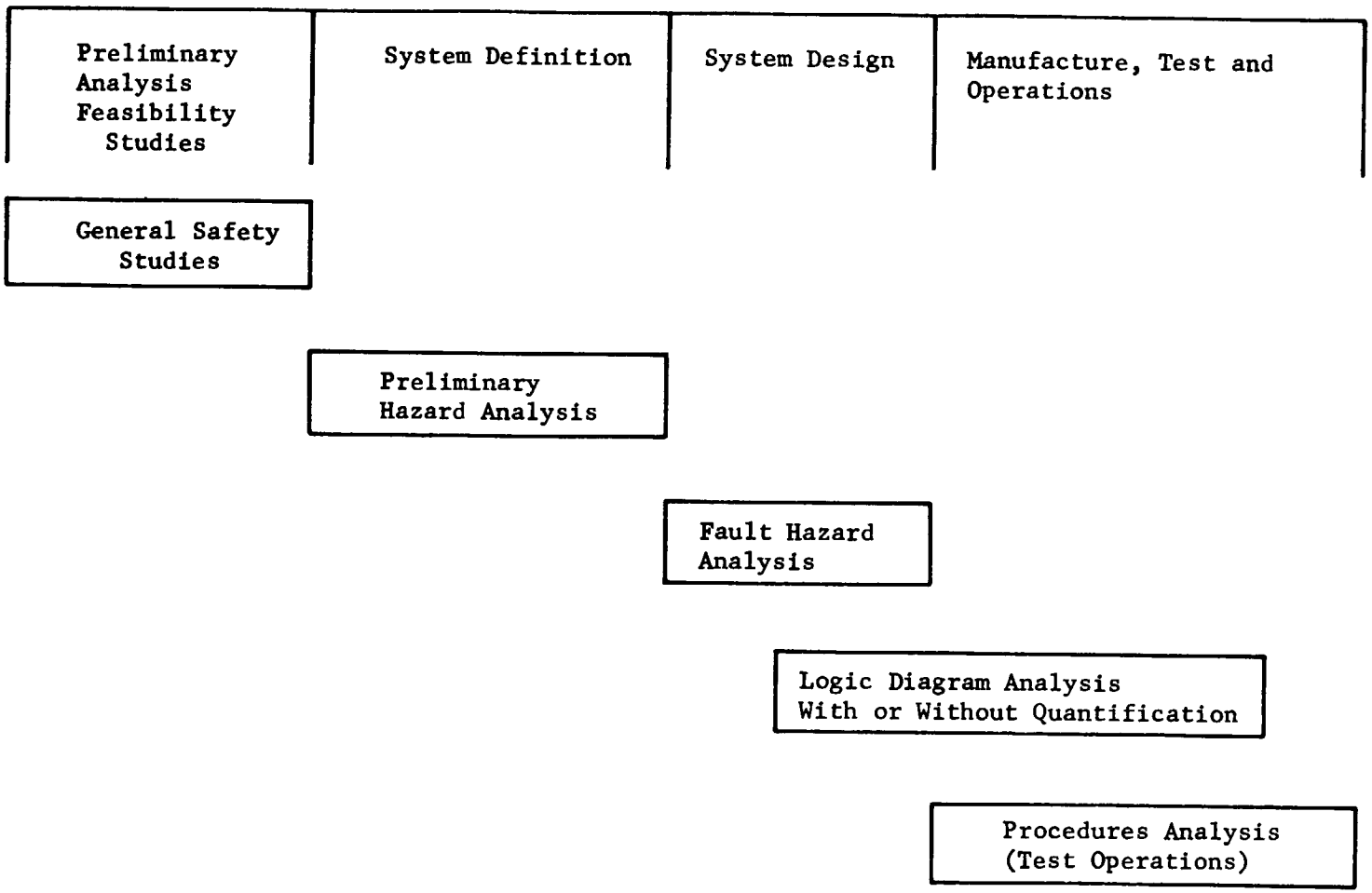


Figure 5

b. A review of all pertinent data related to the evolving system as a means of learning the system.

c. A listing of all energy sources such as:

(1) Electrical

(2) Mechanical

(3) Chemical

(4) Nuclear

d. Determining the design features or procedures that have been developed to control the energy sources listed in subparagraph c.

e. Identifying energy sources for which inadequate controls have been adopted, or high risk areas.

f. Identifying safety requirements and criteria incorporated or needed to assure control of the energy sources and documenting them for future program application.

g. Making recommendations to the program manager in cases where inadequate controls exist.

h. Reiterating the process as frequently as required to support major program changes.

i. The use of this information as applicable for an input into trade studies and program reviews.

3. In performing a preliminary hazard analysis, a chronological listing of functions or events provides a basis for defining generic systems. An example listing of mission functions or events with generic systems to perform those functions on an unmanned space vehicle is presented in Figure 6.

4. The next step in the preliminary hazard analysis is to determine the hazards involved with each of the defined generic systems. The hazard determination is based on data and experience from previous programs. For brevity in this hazard analysis example, the listing of hazards for only one of the mission functions is presented. Undesired events and their causes for the generic systems defined from a launch-boost function are presented in Figure 7 together with identified safety features and inadequate controls as a means of determining areas needing further consideration.

3204 FAULT HAZARD ANALYSIS

1. This analysis technique is the second in the series, with increased complexity over the Preliminary Hazards Analysis. A more completely defined system and greater system knowledge are required

UNMANNED MISSION FUNCTION LISTING EXAMPLE

MISSION EVENTS	GENERIC SYSTEMS
LAUNCH-BOOST	Guidance, Fuel, Engines, Destruct Staging, Oxidizer, Flight Control, Electrical, Telemetry
FAIRING SEPARATION	Separation, Electrical
ORBITAL INJECTION	Engine Shutdown, Payload Separation, Electrical, Guidance
SOLAR PANEL DEPLOYMENT	Squib, Unfolding, Electrical
ATTITUDE POSITIONING	Reaction Control, Electrical, Navigation
ORBIT CORRECTION	Propulsion, Computer, Electrical, Navigation
DATA ACQUISITION	Antenna, Telemetry, Computer, Electrical
MID-COURSE CORRECTION	Propulsion, Computer, Navigation, Electrical
STAR ACQUISITION	Navigation, Reaction Control, Computer, Electrical
DATA ACQUISITION AND TRANSMISSION	Sensing, Data Storage, Telemetry, Electrical

Figure 6

EXAMPLE LISTING OF HAZARDS FROM PRELIMINARY ANALYSIS

MISSION FUNCTION	GENERIC SYSTEMS	UNDESIRED EVENTS	HAZARDOUS CONDITION	SAFETY FEATURES	INADEQUATE CONTROLS
LAUNCH-BOOST	ENGINES	Loss of total stage thrust - vehicle loss	Loss of one engine thrust, engine explosion	Destruct system	No redundancy
	FLIGHT CONTROL	Loss of thrust vectoring - vehicle loss	Hydraulic actuator leak or seizure, erroneous signal	Redundancy	No
	FUEL	Engine shutdown - vehicle loss	Pressure switch fails to actuate, fuel leak	Fuel vent valves	Yes
	OXIDIZER	Engine shutdown	Lox leak	None	Yes
	STAGING (Rocket)	Loss of staging - vehicle loss	Motor case rupture	Destruct system	No redundancy
	GUIDANCE	Loss of flight control - vehicle loss	Receiver or transmitter malfunction	Destruct system	Yes
	ELECTRICAL	Loss of flight control, guidance - vehicle loss	Open circuit, short circuit source or control malfunction	Some redundancy	Yes
	DESTRUCT	Loss of thrust - vehicle loss	Inadvertent actuation	S & A switch with redundancy	Yes
	TELEMETRY	Loss of parameter monitoring - mission degradation	Sensor malfunction	None	Yes
		Loss of space vehicle status monitoring - loss of mission	Transmitter malfunction	None	No

Figure 7

for this analysis since the emphasis is oriented to the appropriate system element level, rather than toward a systems approach. The analysis provides greatly increased visibility from the standpoint of primary and secondary failures, as well as sequential failures, and may be performed either as an extension of the Failure Modes and Effects Analysis (FMEA) or independently from the FMEA. In the event that FMEA's have not been accomplished, a comparable set of data must be developed by the safety analyst before the Fault Hazard Analysis can be completed.

2. The data required for this analysis include up-to-date:

   a. Drawings, specifications and hardware (system) descriptions.

   b. Mission time lines (projected).

   c. Failure modes and effects analyses.

   d. Historical data including test results.

3. The Fault Hazard Analysis (FHA) is used to define the effects of various subsystem component or piece-part failure modes, to evaluate these effects on system equipment or personnel, and to determine which subsystem effects should be further analyzed during subsequent safety analysis. The FHA considers all these system elements in the subsystem and, therefore, all the interface effects resulting from internal failures. Analyzing at the appropriate system element level allows the identifiable hazards to be found, because, in the FHA, each hazardous event must terminate in a subsystem major component.

4. The format shown in Figure 8, which is an extension of the normal FMEA, may be used in performing the Fault Hazard Analysis. The following subparagraphs provide information on the use of this format by reference to column heading:

   a. Component. Components are defined, at the discretion of the analyst, by their physical or functional significance to the subsystem or its design concept, or in accordance with NHB 5300.4(1A), Reliability Program Provisions for Space System Contractors. The following guide for defining the major components is included to facilitate understanding of the types of natural separations to consider. It is not intended to be exhaustive.

      (1) Electronic Logic Circuits. Many components are made up from a small number of basic circuit designs which perform an identifiable purpose. These are used as building blocks for larger circuits designed to perform the required logic functions to the subsystem. To minimize the analysis required, the basic circuits can be defined as major components, and an analysis made of each logic function.

      (2) Mechanical Devices. Mechanical devices can be either a single part or an assembly of parts which perform one function. For a Fault Hazard Analysis, a major mechanical component can be defined as either of these. The use in the circuit will dictate

TYPICAL FM&EA DATA SHEET REVISED

FAULT HAZARD ANALYSIS

COMPONENT	COMPONENT FAILURE MODE	COMPONENT FAILURE RATE (PRIMARY)	SYSTEM OPERATIONAL MODE	EFFECT OF PRIMARY COMPONENT FAILURE ON SUBSYSTEM	FACTORS THAT MAY CAUSE SECONDARY COMPONENT FAILURE	UPSTREAM COMPONENTS OR INPUTS THAT MAY CAUSE SEQUENTIAL FAILURES	FURTHER ANALYSIS REQUIRED	REMARKS
A	B	C	D	E	F	G	H	I

STANDARD FM&EA ANALYSIS DATA

SYSTEM SAFETY FAULT HAZARD ANALYSIS DATA

Figure 8

to what level of detail mechanical parts should be considered. Single parts which might be considered major components are: solid drive shafts, engine blocks, primary structure, etc. The majority of mechanical devices will be assemblies of many parts and it is more reasonable to treat the assemblies as major components. For example: relays, pumps, motors, mechanical safety devices, and other similar devices. This permits the majority of vendor supplied mechanical devices to be analyzed as major components, thus avoiding the requirement for vendors to provide Fault Hazard Analyses of their subsystems.

(3) Electrical Systems. Major components can be basic components of a circuit or combinations of components (such as amplifiers, rectifiers, or regulators) used to perform one single function. The level of analysis should be based on the importance of the part as a functional element in the design.

(4) Chemical Systems. In systems containing chemical compounds, the chemicals should be considered as major components if these compounds can cause failures of other components through chemical reaction or release of chemical energy. Examples of chemical components are: fuels, pressurants, coolants, and preservatives.

(5) Safety Devices. Safety devices should always be considered major components since they are used primarily to protect against undesired events.

(6) Wiring. Interconnecting wiring of major components may be considered a major component. Internal wiring can be considered as a part of a major component. Physical characteristics of cables which circumvent failures between wires should be stated in the cable analysis.

b. Component Failure Mode. Failures of major components consisting of one part require a listing of the modes in which that part may fail. Failures of major components consisting of more than one part will require a failure mode and effects reliability analysis to determine how the failure modes of each part will affect the components' output. These effects will be the failure modes of the major component listed in the Fault Hazard Analysis. All failure modes of the component must be listed.

c. Component Failure Rate. The predicted reliability or the failure rate computed from the best available data of primary failures should be tabulated in this column for each major component in each of its modes of failure. These data can be used in evaluating probability of the fault event or in selecting which critical or catastrophic events should be analyzed if the decision is made not to analyze all events so classified. These data also serve as a data bank for future reference when the need arises to analyze other undesired events as a result of system changes.

d. System Operational Mode. Many major components are only recurrently activated during the system's operational life. The level of stress of these components will change from one system mode to another. The effect of a failure in each mode can be different; for example, components supplied with power only during a test can create a fault hazard only while a test is performed. Failures existing in one mode of system operations can also adversely affect the system when the mode is changed. Therefore, each major component failure mode must be analyzed for possible effects on all system operational modes.

e. Effect of Primary Component Failure on Subsystem. The effect of the component's abnormal output on the operation is listed in this column. The effect will be of the immediate functional output on the most proximate downstream components. No secondary considerations are necessary. A description of the functional effect on normal subsystem operation will supply the required information. Some failures can initiate a normal chain of events within the subsystem. Those sequences that are inherent to the design can also be reported as a primary effect. The description of the subsystem effect should be identified by its particular oriented function and also by form and magnitude of output energy. This information is necessary when using the completed Fault Hazard Analysis for construction of the Logic Diagram Analysis. Once an undesired event has been defined, all primary failure modes can be found by scanning this column.

f. Factors That May Cause Secondary Component Failure

(1) Any major component operating in a system is subject to out-of-tolerance or abnormal inputs. There may be no source of such conditions within the subsystem under analysis, but once integrated into a system, abnormalities can arise. To insure detection of the hazardous secondary conditions which can cause equipment failure, the limits beyond which failure occurs will be listed. This information is very significant, because a failure causing an out-of-tolerance condition can affect many critical system functions simultaneously and may degrade the system's safety.

(2) The following information, where applicable, should be included in this column:

(a) Effect of power reversals.

(b) Effect of high and low power.

(c) Temperature and moisture limits.

(d) Shock limits.

(e) Vibration limits.

(f) RFI limits.

(g) Electromagnetic limits.

(h) Transient effects.

(i) Chemical effects (including corrosion).

(j) Any other source of energy which, if supplied in sufficient quantity, will cause the primary failure rate to increase.

g. Upstream Components or Inputs that May Cause Sequential Failures. The analysis cannot be continued unless it is known how the out-of-sequence event could occur due to the power functioning of the component. It was shown above that a fault effect on a subsystem may be caused by a primary or secondary failure on a component. This column shows how the fault effect on the subsystem may be caused by the component as the result of having improper input signals applied. This is termed a "sequential failure" and describes the specific subsystem oriented functions and their energy level required to cause the out-of-sequence failure mode. Improper outputs of the most proximate upstream components should be listed.

h. Further Analysis Required. Having completed the analyses necessary to fill out the preceding columns, the analyst is prepared to make recommendations on the necessity for additional analyses or corrective action. The basis for these recommendations is the result of reviewing the data developed against the risk factors of severity, exposure and probability of occurrence as cited previously, and a yes or no decision is reached which is entered in Column h with appropriate remarks added to Column i.

i. Remarks

(1) This column is used to include additional information needed to clarify or verify information in the other columns, or to provide a permanent note of recommended future action. A few examples of usage are given below:

(a) Describe the number and type of monitors on this major component failure mode, if known.

(b) Show the recommendations for further system analysis or corrective action as a permanent note.

(c) Explanation of a major component definition in doubtful cases.

(d) A coding to show data source and validity of the primary failure rates.

(e) A discussion of sequential failure events is entered in Column g.

(f) When applicable, a statement that the major component is an interface component and requires an input from another subsystem or can provide the abnormal output in Column e.

(2) When the decision is made not to proceed into the logic diagram analysis, the product of the Fault Hazard Analysis -- which is included in Columns g and h of the tabulation -- may be used as follows:

(a) To provide visibility as to the relative safety at the subsystem level.

(b) To establish the need for additional design requirements, safety devices, control procedures or mission constraints (red line values).

(c) As background safety data for support of design reviews to assure that safety requirements have been met.

(d) As the basis for safety support of trade-off studies.

3205 LOGIC DIAGRAM ANALYSIS

1. GENERAL

The logic diagram analysis technique is the final progressive step in the series of safety analyses. The effort can be undertaken in increments as the major subsystem configurations are defined; however, the complete system configuration must be established before the total analysis can be accomplished. The analysis is flexible and provides maximum visibility for the total system viewpoint by clearly showing the critical fault paths that exist in the system, which are not revealed by the previously described analytical techniques.

2. METHOD

A logic diagram is a graphic representation of the various parallel and series combinations of subsystem failures which can result in a predetermined system failure. The accomplishment of a Logic Diagram Analysis is undertaken in the following series of steps:

a. Definition of the Undesired Event. Every system developed has one or more events which that system cannot tolerate, such as a catastrophic loss of a system, loss of a crew, or loss of a mission. It follows then that these are the events which must be prevented from occurring; and, in turn, prevention of these events becomes the objective of the logic diagram analysis. The initial step in the performance of a logic diagram analysis is the definition of the event which must be kept from happening. While the definition of these undesired events may originate from within the functional safety organization, senior management concurrence should be obtained as a prerequisite to begin the analysis.

b. Obtain Data That Describes the System and Its Planned Use:

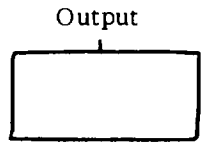
(1) Update the data obtained for the Fault Hazard Analysis to the current baseline.

(2) Develop cognizance of all significant changes to the system baseline.

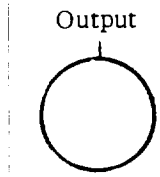
c. Develop the Logic Diagram. Once the predetermined event has been established as described in subparagraph a above, determine the necessary parallel and series events which will cause the end event to occur. This process is continued through the subsystem level to the appropriate component or piece-part level. In cases of safety critical components, as defined in the Fault Hazard Analysis, the process is always continued to the piece-part level. These series and parallel events are connected by use of the following graphic symbols:

(1) Events. The various kinds of events used in a logic diagram are represented by the following symbols:

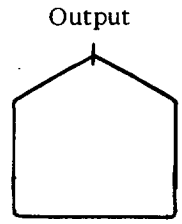
(a) The RECTANGLE identifies an event that results from a combination of fault events.



(b) The CIRCLE identifies a basic failure of a component.



(c) The HOUSE indicates an event which is normal for the system.

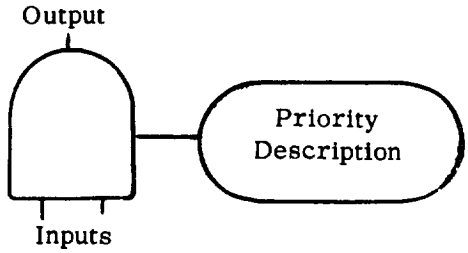


(d) The DIAMOND identifies a failure which has not been fully developed due to lack of information or significance.

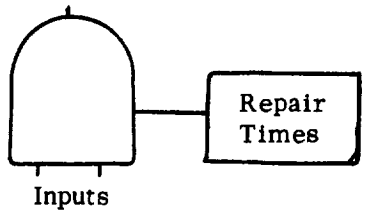
(2) Logic Operators. The logic operators required to develop the logic diagram are defined and symbolized as follows:

(a) The AND GATE describes the logical operation which requires the coexistence of all inputs to cause the output.

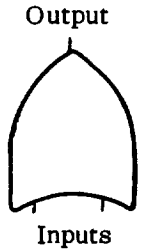
(b) The PRIORITY AND GATE performs the same function as the AND GATE except that the inputs must occur in the sequence stipulated.



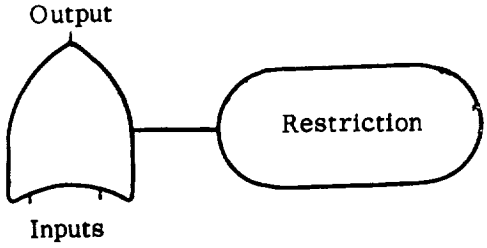
(c) The CONSTANT REPAIR performs the same function as the AND GATE except that the repair time of the output event is not dependent on the repair times of the inputs.



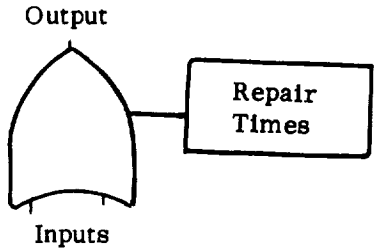
(d) The OR GATE describes the logical operation whereby the output is caused by the occurrence of any of the inputs.



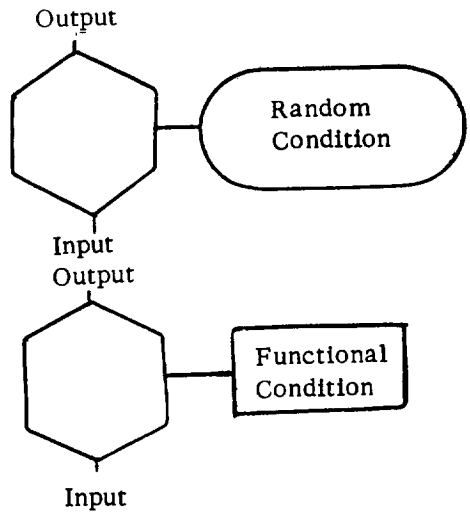
(e) The EXCLUSIVE OR GATE performs the same function as the OR GATE except that specified inputs cannot coexist.



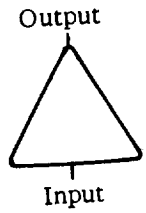
(f) The CONSTANT REPAIR OR GATE performs the same function as the OR GATE except that the repair time of the output event is not dependent on the repair times of the input.



(g) The INHIBIT GATE describes a situation in which a certain condition of the system must exist before one failure produces another. The inhibit condition may be either normal to the system or be the result of equipment failures.

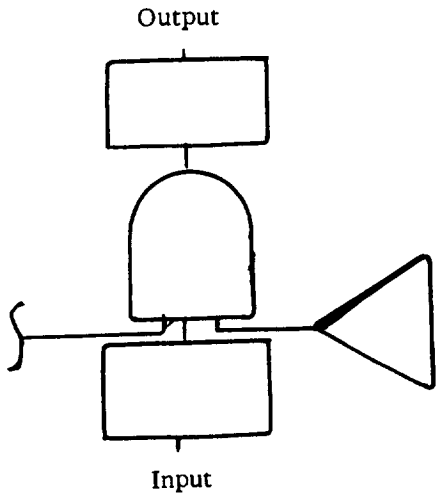


(h) The MATRIX GATE is used to describe a situation in which an output event is produced for certain combinations of events at the inputs. A matrix showing the event combinations that produce the output event will accompany each usage of this symbol.

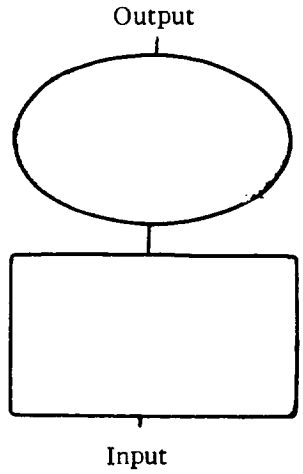


(3) Special Symbols. Special symbols are used in order to simplify the graphic representation of fault tree construction. These special symbols are shown below:

(a) The TRANSFER symbol is used to show continuity between two parts of the tree. A line into the side of the triangle transfers everything below to another area identified by the triangle with a line drawn from the apex.



(b) An ELLIPSE with a line extending out along the major axis is used when a component appears several times at the same place (e.g., at 10 stage counter). Only one of the inputs is drawn and the ellipse is drawn to encompass the output. This indicates that the failure rate of that event is to be multiplied by the given factor for an OR GATE or raised to a given power for an AND GATE.



d. Critical Fault Path Identification

(1) A critical fault path is that chain of events which is the most likely to result in a particular predetermined event or potential accident. There may be several chains of various degrees of dominance. These chains and their associated degrees of dominance are most clearly identified in the system safety model (logic diagram). Critical fault path(s) and their relative degree of dominance are determined either by event weighting (inspection) or mathematical solution of the model.

(2) Since the most critical fault path is the most likely avenue along which predetermined event(s) can occur, the most effective approach is to concentrate the initial corrective action in this area. It may be necessary to consider other paths within the model, in a descending order of dominance, in order to achieve an acceptable level of risk for the occurrence of a particular predetermined event or potential accident.

(3) The steps required to provide effective use of the identification of critical fault paths are as follows:

(a) Assure that the system safety model for a given predetermined event or potential accident has been developed to the extent necessary to identify critical fault paths. As a minimum the logic diagram development must encompass all these safety features and devices which have been designed into the system which may be extracted from the previous analyses. This assures that adequate consideration has been given to those areas of the system which contain the greatest risk. Safety features and devices are normally placed where there exists the greatest risk of an undesired event occurring.

(b) By logical inspection or mathematical process, determine the degree of dominance for those critical fault paths of the model which contribute the most to the risk. Logical inspection is the logical thought process of a trained and experienced analyst being applied through examination of the model. This process, associated with whatever mental weighting factors he may consider during the examination

to determine which events "look to be" more probable than others, would lead to the resulting statement by the analyst: "these events (identified) and critical fault path(s) look to be the most probable." The term "mathematical process" can be a solution of the model by any of several methods. Since the purpose of the quantitative evaluation of a diagram is to evaluate the critical fault paths and establish their relative significance, the diagram is usually simplified by inspection to minimize the logic diagram structure to be evaluated. This inspection results in elimination of those events and branches which are obviously insignificant compared to others which are inputs to the same gate.

(c) Evaluate the dominant critical fault paths by accomplishing the following steps:

(i) Establish a predetermined limit within which the initial path selection is bounded. This involves the identification of those paths which are computed to be above any established limit for the system. If the paths are near or below the limit, then they are selected by picking those which are within an "order of magnitude" or so of the limit, or are of the same type.

(ii) The initial selection must be divided into groups for which a set of predetermined limits has been established for each grouping. The grouping of paths is accomplished by selecting those within an order of magnitude of each other or those which have an apparent commonality within the system.

(iii) Determine whether a common point of departure exists among the paths of each group. This evaluation involves determining whether there are common faults among the paths. Recommended changes to the system at these common points provide the most effective way to eliminate critical fault paths, or at least reduce them to an acceptable level of risk.

(iv) Convert the logic diagram dominant critical fault paths by grouping events at logical summary points. Conversion of the logic diagram critical fault paths involves making a listing of those events which when "ored" result in an interim event. The method is to convert each path to a simplified alternating "and", "or", "and", "or", etc., relationship.

(v) Simplify the logic diagram of the dominant critical fault path by logically re-diagramming.

(vi) Determine those events for which a design change or the development of a procedure will best and most cost-effectively reduce the probability of occurrence of an undesired event to an acceptable level of risk.

(vii) System safety trade-off studies may be made by inserting alternative solutions as derived by subparagraphs (i) through (vi) and repeating the process until an acceptable level of risk is obtained. This step involves working with designers and selecting several alternative system changes to reduce the probability of occurrence of each path. For each alternative to be evaluated the logic diagram is changed to reflect the change and the diagram is re-computed to determine the change impact. Care must be exercised to assure that other paths or branches of the diagram which have the same event or fault sequence are also changed to reflect the change being evaluated.

(viii) Advise appropriate level of management of findings and recommendations.

(ix) Diagnostic analyses also may be performed by the use of this technique. The analyst sets the accident that actually happened as his undesired event and develops the diagrams as described in subparagraphs a through c above.

3206 PROCEDURES ANALYSIS

1. GENERAL

The purpose of the procedures analysis is to identify and/or implement the safety requirements that should be met to assure safe test or operation of the system. The data required for the performance of these analyses include:

a. Drawings, specifications and hardware (system) descriptions.

b. Mission time lines or test requirements.

c. Results of all safety analyses previously performed.

d. Historical data from previously performed tests on similar systems.

2. THE SAFETY-PROCEDURES INTERFACE

The safety-procedures interface is established in three steps as follows:

a. Working with the engineering organization, establish specific safety requirements and insert them into the test or operations requirements documentation.

b. Review the test or operations procedures when they have been prepared to verify that the safety requirements included in the test or operations requirements documentation have been included in the procedures. Special attention should be devoted to backout and shutdown capability and to assure the procedures include end-to-end verification.

c. Monitor the actual test or operation to assure the adequacy of the safety impact to the procedures and to assure that the requirements are followed.

Test procedures include developmental, qualification, acceptance and system validation. Operating procedure includes handling, storage, transportation, maintenance, operation and emergency.

3. METHOD

a. This analysis technique involves the review of all operating procedures associated with the program. Emphasis is placed on the completeness of the procedures, including all cautions to be exercised regarding inadvertant out-of-sequence operations, and the inclusion in the procedures of adequate recycle and backout instructions to counter potential emergency situations. Documentation of identified hazards involved with operational and remedial procedures will provide management visibility of the risks involved and corrective action needed for avoiding or reducing the hazards.

b. Analyses consisting of reviews of prepared procedures for the following nonoperational activities in a system development program should include:

(1) Manufacturing

(2) Personnel Skill Certification

(3) Test

(4) Transportation

(5) Storage

(6) Pre-Operation Checkout

(7) Maintenance

c. Figures 9 and 10 are typical checklists that contain hazard examples that may benefit the safety analyst in performing procedures analyses.

3207 REQUIREMENTS VERIFICATION

1. The product of the analytical safety effort consists of safety visibility used in support of risk managenent decisions and safety requirements used to influence design or procedures that test or operate the system. It is necessary not only to establish the initial safety requirements and criteria, but to evaluate these requirements and criteria on an iterative basis to assure they accomplish the intent for which they were originated. Moreover, new requirements may be developed or existing requirements changed in order to maintain the established safety level of the system.

TYPICAL TEST CHECKLIST

POTENTIAL PROCEDURAL HAZARD	INDUSTRIAL SAFETY INTERFACE	POTENTIAL EFFECT
PERSONNEL (OPERATOR) HAZARDS		
Procedures in error.		Unmeasurable product integrity from deviations? improvisions.
Procedures omissions (steps and conditions).		Unmeasurable product integrity from deviations/ improvisions.
Procedures out of sequence.		Unmeasurable product integrity from deviations/ improvisions.
Procedures warnings and cautions inadequate.		Undetectable product effects from exceeding process limits.
Procedures permissible alternative sequences.		Undocumented conditions/product integrity.
Procedures sketches, diagrams, test points in error.		Undisclosed product integrity from invalid test data.
TEST EQUIPMENT HAZARDS		
Shutdown procedures inadequate (normal and emergency).	X	Unmeasurable product/test equipment degradation.
Indicating/warning devices ineffective.		Unmeasurable product/test equipment degradation.
Maintenance/calibration reqmts/schedule uncontrolled.		Invalid test compliance/qual. and reliability integrity.
Automatic corrective devices malfunction.		Unmeasurable product degradation/operational limits exceeded.
Inadequate interlocks for sequential events.		Unmeasurable product degradation/operational limits exceeded.
Inadequate protection for product:		
High voltage.	X	Unmeasurable product/test equipment degradation by overexposure.
Electromagnetic and radio frequence interference.	X	"
X-ray, nuclear radiation.	X	"
Heat.	X	"
Acoustic noise, vibration, shock.	X	"
Pressure or vacuum.	X	"
Cryogenics.	X	"

Figure 9

TYPICAL MANUFACTURING CHECKLIST

POTENTIAL PROCEDURAL HAZARD	INDUSTRIAL SAFETY INTERFACE	POTENTIAL EFFECT
PERSONNEL (OPERATOR) HAZARDS		
Procedures omissions (steps and conditions).		Unmeasurable product integrity from deviations/ improvisions.
Procedures out of sequence.		Undetectable structural/operational integrity.
Procedures inadequate warnings and cautionsl		Unmeasurable product integrity from exceeding limits.
Procedures omitted back-out or emergency procedures.	X	Unmeasurable product integrity from process improvisions.
MANAGEMENT RELATED HAZARDS		
Use of non-certified personnel.		Invalid product qual. and reliability assurance.
Insufficient supervision and inspection.		Unmeasurable product integrity/deviations and improvisions.
Inadequate critical incident reporting.	X	Untraceable events and conditions negate corrective action.
MANUFACTURING EQUIPMENT HAZARDS		
Devices and instruments not calibrated.		Unmeasurable product effects/process parameters in error.
Special tooling/equipment not provided.		Unmeasurable product effect/deviation and improvisions.
ENVIRONMENTAL HAZARDS		
Inadequate environment control:		
Presence of corrosive gases, particulate matter.	X	Undetectable product exposure and degradation.
Temperature extremes.	X	Undetectable product exposure and degradation.
Humidity extremes.	X	Undetectable product exposure and degradation.
Excessive noise, vibration, shock levels.	X	Undetectable product exposure and degradation.

Figure 10

2. Original safety requirements and criteria stem from data extracted from experience gained on similar systems, standard system safety technology and the preliminary hazards analysis. More detailed safety analysis such as the fault hazard analysis and the logic diagram analysis will yield requirements that are unique to the evolving system.

3. Concurrently with the performance of these analyses, the original safety criteria should be assessed to verify that these requirements correctly continue to influence the design as it evolves. It is essential, as these safety requirements are developed or refined, that they be documented and that this documentation be maintained on an up-to-date basis for design use.

APPENDIX A: INSTALLATION SUPPLEMENTAL INSTRUCTIONS AND REQUIREMENTS

1. In order that all regulations concerning various aspects of the NASA Safety Program (i.e., agency and installation) are maintained in one publication, the volumes of the NASA Safety Manual have been designed so that installation supplements will be issued and filed with the basic regulations.

2. Installations will issue, as Supplements to each volume, their implementing instructions in a format similar to that indicated in Exhibit A of this Appendix. The installation Supplements will be issued as page inserts to those paragraphs needing implementation and will be filed as near to the implemented paragraph as possible. The implementing instructions will be printed on color paper stock.

3. The Cover Sheet for each Supplement will be in a format similar to that indicated in Exhibit B and will contain the following information:

   a. A list of the basic paragraphs being implemented.

   b. A synopsis, if helpful, of the new implementing instructions.

   c. A statement that basic paragraphs should be annotated "See _____ Sup. _____."

4. In the sample formats in Exhibits A and B, the abbreviation "NHQ" designates "NASA Headquarters." Field installations should use individual designations (e.g., "MSC" for Manned Spacecraft Center, "FRC" for Flight Research Center). Headquarters Supplements will be printed on green paper.

5. In no case will this volume be reproduced or reprinted in any manner.

NHQ Sup. 1.

Effective Date: _____

NASA HEADQUARTERS SUPPLEMENT 1
to
NASA Safety Manual
(NHB 1700.1(V3))

1. NHQ 3302-2a(2)(c)(i)

(Include installation supplemental procedures only)

NHQ Sup. 1. (Page Number)

EXHIBIT A--SUPPLEMENT

NHQ SUPPLEMENT 1
to
NASA Safety Manual
(NHB 1700.1(V3)
Issue Date: _____

This Supplement contains NASA Headquarters (NHQ) implementation of basic paragraphs 1302, 3401 and 3504. These paragraphs should be annotated "See NHQ Sup. 1."

NHQ 3032 Requires processing of NHQ. Form 00 through Code BN.

FILING INSTRUCTIONS

1. (Include appropriate instructions for filing.)

EXHIBIT B--COVER SHEET

APPENDIX B: SYSTEM SAFETY REFERENCES

NASA

SAFETY PROGRAM DIRECTIVE NO. 1	SYSTEM SAFETY REQUIREMENTS FOR MANNED SPACE FLIGHT, OMSF, WASHINGTON, D.C.
NASA TM-X 53282	LAUNCH VEHICLE SAFETY ENGINEERING FOR STANDARD PAYLOAD MODULE, OCTOBER 20, 1965, MSFC
NASA TM-X 53612	THE SYSTEMS SAFETY PROGRAM FOR A TOTAL SPACE LAUNCH VEHICLE GENERAL REQUIREMENTS, MAY 23, 1967, MSFC
NASA TM-X 53305	STANDARD PAYLOAD MODULE SYSTEM ANALYSIS PROCEDURES FOR SYSTEM DEFINITION, JULY 26, 1965, MSFC
NASA TM-X 53664	SYSTEMS SAFETY CRITERIA FOR USE IN PREPARATION OR REVIEW OF PROCEDURES, OCTOBER 17, 1967, MSFC
NASA TM-X 53563	SYSTEM SAFETY HANDBOOK, JANUARY 6, 1967, MSFC
NASA TM-X 53388	SATURN V SYSTEM SAFETY PROGRAM ADEQUACY EVALUATION, FEBRUARY 1, 1966, MSFC
NHB 5300.4(1A)	RELIABILITY PROGRAM PROVISIONS FOR SPACE SYSTEM CONTRACTORS, R&QA, CODE KR, WASHINGTON, D.C.
SP 6506	AN INTRODUCTION TO THE ASSURANCE OF HUMAN PERFORMANCE IN SPACE SYSTEMS, R&QA, CODE KR, WASHINGTON, D.C.

DOD

AFSC DH 1-1	DESIGN HANDBOOK
AFSC DH 1-6	DESIGN HANDBOOK, "SYSTEM SAFETY" (Also reference listed herein.)
AFSCM 127-1	SYSTEM SAFETY MANAGEMENT
AMCP 385-23	MANAGEMENT SYSTEM SAFETY
MIL-STD 882	SYSTEM SAFETY PROGRAM FOR SYSTEMS, AND ASSOCIATED SUBSYSTEMS AND EQUIPMENT: General Requirements for

AFETRM 127-1 RANGE SAFETY MANUAL (VOLUME 1)

AFSCM 127-1 SAFETY, SYSTEM SAFETY MANAGEMENT, AIR FORCE SYSTEMS COMMAND

SAMSOM 127-1 SAFETY, PLANS, PROGRAMS AND PROCEDURES (Volume IV), SYSTEM SAFETY ENGINEERING, SPACE AND SYSTEMS ORGANIZATION MANUAL, USAF

EXHIBIT 68-8 WEAPONS SYSTEMS SAFETY ANALYSIS REQUIREMENTS, SAMSO-AFSC, LOS ANGELES, CALIFORNIA, NOVEMBER 1968

SAMSO SYSTEM SAFETY ENGINEERING, HAZARD ANALYSIS REQUIREMENTS, SAFETY OFFICE (SMW) SAMSO-AFSC, LOS ANGELES, CALIFORNIA, JULY 1968 (MAJOR P. J. STACK)

CONTRACTOR

D2-117018-1 APOLLO LOGIC DIAGRAM ANALYSIS GUIDELINES, THE BOEING COMPANY, SEATTLE, JUNE 1968

D2-84303-1 SYSTEMS SAFETY ENGINEERING ANALYSES TECHNIQUES, THE BOEING COMPANY, SEATTLE, FEBRUARY 1963

D2-119062-1 SYSTEM SAFETY ENGINEERING ANALYSIS HANDBOOK, THE BOEING COMPANY, COCOA BEACH, FLORIDA, JUNE 1969

APPENDIX C: TRAINING COURSES

COURSE NO.	TITLE	SCHOOL	DURATION
104	System Safety	George Washington Univ. Washington, D.C.	2 weeks
-	System Safety Analysis	University of Washington Seattle, Washington	2 weeks
ASM 576	Fundamentals of System Safety	University of Southern California, Los Angeles	3 weeks
ASM 577	Aeronautical Systems Safety	University of Southern California, Los Angeles	3 weeks
ASM 578	Missile and Space Vehicle Systems Safety	University of Southern California, Los Angeles	3 weeks
ASM 579	System Safety Technology	University of Southern California, Los Angeles	3 weeks
	Advanced Safety Program Management	University of Southern California, Los Angeles	3 weeks

GPO 889-573